УДК 621.391.7:336.71(075.8)

В.К. Задірака, А.М. Кудін, В.О. Людвиченко, О.С. Олексюк
Інститут кібернетики ім. В.М. Глушкова, м. Київ, Україна
zvk140@ukr.net

Спеціальні цифрові носії інформації – теорія, технології, застосування

Стаття присвячена питанням реалізації криптографічних механізмів захисту в автоматизованих системах. Розглядається запропонована авторами теорія «спеціальних цифрових носіїв інформації», яка дозволяє практично повністю відокремити розвиток засобів обробки даних від засобів криптографічного захисту даних та створити універсальну програмну платформу для захисту будь-яких електронних документів. Наводяться переваги даного підходу перед існуючими, перспективи розвитку запропонованої теорії, аспекти її практичного застосування.

Вступ

У процесі розвитку суспільства поступово переходять від традиційних форм збереження цінних інформаційних даних (паперових документів суворої звітності, грошей, векселів тощо) до їх електронних аналогів. При цьому спостерігаються наступні тенденції:

− інтеграція електронних аналогів цінних інформаційних даних в рамках програм «електронної держави» («електронного уряду», електронних виборів, електронного документообігу тощо), які передбачають переведення державних органів на «безпаперове» діловодство;
− уніфікація формату електронних документів, які містять цінну інформацію (цифрові сейфи, цифрові паспорти, цифрові цінні папери, гроші);
− уніфікацію технології обробки електронних документів, в тому числі – за рахунок віртуалізації [1];
− уніфікація механізмів захисту інформації (як на рівні криптографічних алгоритмів, так і технологій реалізації) для інформаційно-обчислювальних систем різного класу – від серверів до інтелектуальних карток та кишенькових комп’ютерів;
− випереджальний розвиток інформаційно-обчислювальних технологій порівняно із технологіями захисту інформації.

Останні тенденції визначають необхідність створення нових підходів до захисту електронних документів, які не накладають обмежень на технологію оброблення інформації в сучасних розподілених системах. Одним із таких підходів є запропонована авторами методика «спеціальних цифрових носіїв інформації» [2].

Спеціальні цифрові носії інформації та їх функції

Спеціальні цифрові носії інформації – це електронні документи, що мають містити інформацію, яка є основою для створення систем електронного документообігу, електронної торгівлі та електронного бізнесу (електронні гроші, електронні цінні папери), а також спеціалізовану інформацію для ідентифікації і автентифікації суб’єктів цих систем (наприклад, цифрові паспорти) та спеціальну службову інформацію, яка повинна забезпечити захищену взаємодію з цими електронними документами.

Передумовою появи нової концепції «спеціального цифрового носія» стало створення:

− універсальної програмної платформи для засобів обчислювальної техніки – Java-машини;
− універсальної мови опису даних XML;
− стандартизації криптографічних примітивів захисту інформації.

Розвиток цих трьох напрямків викликав революційні зміни на ринку засобів захисту інформації, зокрема появу технологій BSAFE RSA фірми Data Security [3], PGP Disk, BestCrypt фірми Jetico, DriveCrypt, які продовжують розвиватися в наступних напрямках:

− поступовий перехід від технології криптографічного захисту окремих файлів або записів в інформаційних сховищах до захисту спеціальних носіїв інформації (захищених логічних дисків) та визначених областей оперативної пам’яті;
− відмова від орієнтації на особливості конкретних програм обробки даних, створення універсальних як за інтерфейсами (PKCS#11, Microsoft CryptoAPI тощо), так і за реалізаціями (під різні операційні системи, з використанням технологій Java або аналогічних їй) засобів криптографічного захисту інформації;
− перехід від забезпечення тільки окремо конфіденційності та цілісності даних, що зберігаються в захищеному середовищі (так званих «цифрових сейфів»), до достатньо функціональних логічних аналогів засобів криптографічного захисту інформації, які управляються вибраною політикою безпеки (наприклад, так звана концепція Policy-Based Approach [4]).

Практично йдеться про новий підхід в технологіях реалізації криптографічних засобів захисту даних, а саме – оформлення «програмного прошарку», який реалізує всі необхідні криптографічні механізми захисту практично незалежно від програмно-апаратної платформи реалізації цих механізмів.

Все це дало можливість авторам висунути ідею спеціального цифрового носія, який дозволяє практично повністю відокремити розвиток засобів обробки даних від засобів криптографічного захисту даних та створити універсальну програмну платформу для захисту будь-яких електронних документів. Прикладом переваги такого підходу є вирішення проблеми цифрового підпису електронних документів незалежно від їх способу представлення (кодування, формату та інше). Зауважимо, що класичним аналогом такого універсального захищеного носія є бланки документів суворої звітності з елементами технологічного захисту (наприклад, папір із водяними знаками).

Ідея полягає в наступному. Вводиться поняття «спеціальний цифровий носій» як технологія, яка складається:

– з універсального програмного інтерфейсу для прикладних програм (подібно до Microsoft CryptoAPI);
– множини атомарних програмних модулів (наприклад, Java-аплетів) реалізації криптографічних (стеганографічних) примітивів роботи із блоками даних (шифрування, виробка цифрового підпису, обчислення геш-коду, обчислення імітовставки, обчислення примітиву автентифікації, поставлення цифрового водяного знаку, верифікація цифрового водяного знаку тощо);
– невпорядкованого набору атомарних даних, які можуть бути розташовані на будь-якому фізичному носії та в будь-якому місці розподіленої обчислювальної системи (як в захищеному, так і відкритому вигляді);

– XML-шаблону електронного документа, який і визначає конкретний тип документа (цифровий паспорт, електронні гроші, електронна монета, електронний цінний папір тощо), а також порядок збору документа з невпорядкованого набору атомарних даних і використання для доступу до них атомарних програмних модулів (з точки зору теорії захисту інформації цей шаблон є формалізованою політикою безпеки по роботі з даним електронним документом, портативним інтелектуальним носієм інформації, а з точки зору криптографії – формалізованими правилами застосування криптосистеми);
– універсальної програми-середовища, яка інтерпретує XML-документи (парсер XML-документів) та виконує атомарні програмні модулі (подібно до віртуальної Java-машини);
– програмних інтерфейсів роботи з фізичними пристроями-носіями атомарних даних (наприклад, PKCS#11 – з інтелектуальними картками, USB-токенами, драйверами та програмами роботи з кишеньковими комп'ютерами).

Прикладна програма обробки даних працює тільки з функціями програмного інтерфейсу високого рівня, наприклад Microsoft CryptoAPI, і не змінюється навіть при зміні форми представлення даних, появі нових вимог до їх захисту і навіть при зміні форми документа або переліку документів, які вона обробляє.

Алгоритмом збору та алгоритмом доступу до конкретного електронного документа є XML-документ, який містить опис даних електронного документа та програми (посилання на програми) обробки цих даних. Таким чином, електронний документ «збирається» тільки в необхідний момент часу, при додаванні/модифікації окремих полів електронного документа змінюються тільки XML-шаблон та додаються відсутні атомарні дані або атомарні програмні модулі.

Універсальне програмне середовище (наприклад, віртуальна Java-машина із XML-парсером) інтерпретує XML-документ та виконує атомарні програмні модулі відповідно до обраної політики безпеки. Таким чином, утворюється єдина реалізація роботи з цінними даними для будь-якої програмно-апаратної платформи – єдина реалізація для ПЕОМ, кишенькових комп'ютерів, інтелектуальних карток, USB-токенів тощо.

Даний підхід дозволяє застосовувати достатньо просту формальну модель опису для забезпечення гарантованого доказу рівня безпеки. Так, будь-який засіб захисту інформації представляється як суперпозиції «атомарних» множин:

F – множина «примітивних» (атомарних) механізмів захисту. Прикладом такого механізму може бути реалізація окремого криптографічного примітиву за допомогою Java-технології (Java-applet),

M – множина невпорядкованих даних, які підлягають захисту. При цьому множина M додатково розбивається на підмножини $M = \bigcup_{i=1}^{n} M_i$. Конкретне повідомлення (наприклад, ідентифікатор, який підлягає захисту), є підмножиною $\widehat{M} \subseteq M$. При цьому, як правило, утворення повідомлення без знання «порядку» (або шаблону) є складною обчислювальною задачею;

S – множина «шаблонів» або «операцій» над множинами M та F. Практичною реалізацією цієї множини є XML-документи, а за допомогою XML-мови формується спеціальна мова саме для опису цифрових захищених носіїв інформації – Ukraine Security Language (USL).

Практично S визначає групу підстановок скінченої довжини над множиною M. Декартові множення $< M, F >$ із введеними над ними підмножинами операцій з S саме і описують конкретний засіб захисту інформації.

Застосування та переваги технології спеціальних цифрових носіїв інформації

За своєю природою спеціальні цифрові носії інформації (СЦН) є електронними документами спеціального типу з певним інтерфейсом доступу до них, і тому можуть зберігатися на будь-яких носіях інформації.

Найбільш зручними для указаних вище цілей є портативні інтелектуальні носії інформації, якими є: інтелектуальні картки (інтелектуальні пластикові картки з пам'яттю), токени, кишенькові комп'ютери (або близькі до них за функціональністю смартфони). В останній час як самостійні пристрої збереження СЦН можуть розглядатися засоби реалізації технології електронного паперу [5]. Аналізу властивостей портативних інтелектуальних носіїв інформації присвячена численна література (наприклад, [6]). Оскільки технологія СЦН включає як одну зі своїх складових різновид технології віртуалізації застосувань [7], то може використовувати будь-які з цих інтелектуальних носіїв інформації. Віртуалізація застосувань використовується для технології СЦН і як засіб автоматичного конфігурування під різні програмні платформи (операційні системи).

Переваги запропонованої технології полягають у наступному.

1. Просто та прозоро реалізуються багаторівневі системи захисту та поетапне нарощування системи захисту. В разі необхідності просто змінюються XML-шаблони та додаються атомарні дані (атомарні програмні модулі) без змін прикладних програм обробки даних, реалізації політики безпеки, інших атомарних даних, XML-шаблонів інших користувачів.
2. Підвищується захищеність самих електронних документів за рахунок неструктурованого зберігання даних (методи захисту типу «розділення/збір»).
3. В рамках запропонованої технології існує достатньо простий формальний опис засобів захисту інформації, який дозволяє визначити рівень стійкості до атак із застосуванням доказового підходу.
4. В цілому в системі забезпечується економія зовнішньої пам'яті за рахунок збору необхідних документів тільки в необхідний момент часу.
5. Забезпечується простота модифікації систем захисту (наприклад, при додаванні нових типів документів, за якими забезпечується контроль доступу, додається лише назва XML-шаблону документа, а при додаванні додаткової функції захисту цифрового паспорта (наприклад, цифрових водяних знаків), додаються лише атомарні дані, атомарні програмні модулі та XML-шаблон документа без зміни логіки роботи прикладних програм та інших програмних модулів).
6. Забезпечується максимальна незалежність реалізації електронного документа від фізичних засобів його збереження та обробки.

Подальший розвиток технології СЦН

Перспективними напрямками досліджень в рамках технології спеціальних цифрових носіїв є:

1. Розробка формального опису СЦН для різних класів засобів захисту із урахуванням необхідності захисту від методів криптоаналізу за непрямими каналами [8].

2. Дослідження стійкості методів розподілу інформації. Як формальну модель розподілу інформації можна застосовувати добре розвинуту теорію шифрів перестановки [9], із урахуванням, що символами алфавіту є лексеми відкритого тексту довільної (або такої, що обирається) довжини.

3. Дослідження мінімальних за складністю (при визначених вимогах до стійкості) криптографічних примітивів [10].

4. Дослідження формальних моделей синтезу криптографічних протоколів з визначеною множиною криптографічних примітивів.

Література

1. Campbell S., Jeronimo M. Applied virtualization technology. Usage models for IT professionals and software developments. – IntelPress, 2006. – 252 p.
2. Задірака В.К., Кудін А.М., Людвиченко В.О., Олексюк О.С. Комп’ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: Навчальний посібник. – Київ; Тернопіль: Підручники і посібники, 2007. – 272 с.
3. Kriese K., Finkelstein F. Building of network of trust for Web services with RSA BSAFE Secure Web Services for Java Platform. – Режим доступу: www.rsa.com
4. Bagga W., Molva R. Policy-based cryptography and application. – Режим доступу: www.citeseer.com
5. Каминская Л. Электронная бумага: из мира научной фантастики – в реальность. – Режим доступа: http://itc.ua
6. Пластиковые карты / Быстров Л.В., Воронин А.С., Гамольский А.Ю. и др. – 5-е изд., перераб. и доп. – «БДЦ-пресс», 2005. – 624 с.
7. Чеппелл Д. Виртуализация для Windows: обзор технологий. Microsoft, 2007. – 30 с. – Режим доступа: www.microsoft.ru
8. Жуков А.Е. Криптоанализ по побочным каналам. – Режим доступа: http://www.ruscrypto.ru/
9. Bellare M., Boldyrevay A. The security of chaffing-and-winnowing. – Режим доступу: www.citeseer.com
10. Krause M., Lucks S. On the minimal hardware complexity of pseudorandom function generators. – Режим доступу: www.citeseer.com

В.К. Задирака, А.М. Кудин, В.О. Людвиченко, О.С. Олексюк

Специальные цифровые носители информации – теория, технологии, применение

Статья посвящена вопросам реализации криптографических механизмов защиты информации в автоматизированных системах. Рассматривается предложенная авторами теория «специальных цифровых носителей информации», которая позволяет практически полностью разделить средства обработки данных от средств их криптографической защиты и создать универсальную программную платформу для защиты любых электронных документов. Приводятся преимущества данного подхода перед существующими, перспективы развития предложенной теории, аспекты ее практического применения.

Стаття надійшла до редакції 09.07.2008.